

АНАЛИЗ ЗАЩИЩЕННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В СИСТЕМАХ ЭДО

¹Басыров Р.Р., ¹Паршин К.А.

¹ ФГБОУ ВПО Уральский Государственный университет путей сообщения, Екатеринбург, Россия (620034 Екатеринбург, ул. Колмогорова, 66), e-mail:rrbasyirov@usurt.ru, kparshin@usurt.ru

Аннотация: Настоящая статья посвящена анализу защищенности электронных документов в информационных системах электронного документооборота. Рассматриваются основные специфичные процессы обработки информации содержащейся в электронном документе. Произведен анализ угроз информационной безопасности электронных документов и установлена взаимосвязь между основными видами угроз в системах ЭДО. Дана оценка защищенности современных систем ЭДО.

Ключевые слова: Документ, информация, информационная безопасность, угроза, документооборот, реквизит, защита информации, жизненный цикл документа, искажение информации, утечка информации, несанкционированный доступ.

ANALYSIS OF ELECTRONIC DOCUMENTS PROTECTION IN THE EDM SYSTEM

¹Basyrov R.R., ¹Parshin K.A.

¹ Federal Public State-financed Educational Institution of Higher Professional Education The Ural state University of Railway Transport, Yekaterinburg, Russia (620034 Russia, Yekaterinburg, Kolmogorova Street, 66), e-mail:rrbasyirov@usurt.ru, kparshin@usurt.ru

Abstract: This article is devoted to the analysis of electronic documents protection in electronic document management information systems. The basic processing specific information, contained in the electronic document. The analysis of threats to information security of electronic documents and the interrelation between the main types of threats in the EDF system. The estimation of the security of modern EDF system.

Key words: Document, information, information security, threat, document, requisite, information security, document life cycle, the distortion of information, information leakage, unauthorized access.

В связи с бурным информационным развитием общества и производства, в большинстве государственных, муниципальных учреждений, а также многих крупных коммерческих организациях внедряются системы электронного документооборота. Данные системы позволяют разгрузить бюрократическую машину в организации, повысить темпы работы по обработке информации содержащейся в документах, предоставить мобильный доступ к документам, повысить трудовую дисциплину сотрудников за счет автоматизированных средств контроля работы с документами.

Однако при всех положительных результатах использования ЭДО возникают угрозы информационной безопасности присущие всем автоматизированным информационным

системам. Рассмотрим основные виды угроз, относящиеся непосредственно, к информации, содержащейся в документах, обрабатываемых и хранящихся в системах ЭДО. Во-первых, необходимо определить основные процессы, по обработке информации, протекающие в электронном документообороте. Концепция электронного документооборота базируется на идеи автоматизации, всего процесса классического – бумажного документооборота при помощи информационной системы, поэтому рассмотрим именно его. Согласно определению, процесс документооборота заключается в движение документов в организации с момента их создания или получения до завершения исполнения или отправки. [1] Таким образом можно выявить основные процессы обработки информации, протекающие в документообороте:

1. создание документа;
2. получение документа;
3. исполнение документа;
4. отправка документа;

Рассмотрим, какая информация формируется и обрабатывается в каждом из процессов. Процесс основного наполнения документа информацией происходит на этапе создания документа, на всех остальных этапах в документ вносится специальная информация необходимая и для каждого последующего этапа движения документа (жизненного цикла документа).[6] Информацией формируемой в процессе создания документа, являются: во-первых, реквизиты документа, позволяющие: идентифицировать автора и адресата документа, установить лицо ответственное за придание документу юридической силы, определить наличие ограничений на доступ к документу, определить связность документов; во-вторых, непосредственно текст документа, отражающий его основную содержательную часть, в-третьих согласование документа, содержащее данные о сотрудниках и процессе визирования проекта документа.

К информации, добавляемой в процессе получения документа, относятся сведения о получении документа адресатом. К информации, добавляемой в процессе исполнения документа, относятся: резолюция – информация, отражающая указания по исполнению документа, должностное лицо выдавшее резолюцию, исполнителей резолюции; отметки о наличии контроля исполнения документа. К информации, добавляемой в процессе отправки документа, относятся отметки о дате и способе отправки документа.

Помимо информации, содержащейся в самом документе с точки зрения информационной безопасности, интерес представляет информация обо всех действиях, производимых с документом – история документа, включающая в себя соответствующие отметки о: создании и модификации документа, процессе согласования, подписания, отправки, получение документа конечным исполнителем, исполнение документа. В таблице 1 представлено соответствие видов угроз и информации содержащейся в документах.

Таблица 1. Соответствие видов угроз и процессов обработки информации в ЭДО

Процесс документооборота	Вид информации	Угроза
Создание документа	Реквизиты документа	Искажение информации; несанкционированный доступ
	Согласование документа	
	Содержание документа	Искажение и/или утечка

	История создания и модификации документа	информации; разглашение информации; блокирование доступа (к информации); несанкционированный доступ
Получение документа	Информация о получении документа	Искажение информации; несанкционированный доступ
Исполнение документа	Информация об исполнении документа	Искажение и/или утечка информации; несанкционированный доступ
	История о прохождении документом этапов жизненного цикла	Искажение информации; несанкционированный доступ
	Информация об исполнении документа	Искажение информации; несанкционированный доступ
Отправка документа	История о прохождении документом этапов жизненного цикла	Искажение информации; несанкционированный доступ

Помимо электронного документооборота, почти все современные системы ЭДО реализуют концепцию электронного делопроизводства, включающего помимо документооборота – документирование, оперативное хранение и использование документов. При работе с документом в каждом из этих процессов также формируется определенная информация, нуждающаяся в защите, конкретно это история работы с документом отражающая кто и когда получал доступ для работы с документом и какие действия с документом он производил (чтение, запись, копирование, печать документа). Основными видами угроз для такой информации является искажение и несанкционированный доступ к информации. [2-5]

Исходя из всего вышеперечисленного можно установить, что угрозы разглашения, утечки, изменения содержательной части документа, а также блокирование доступа к ней, формируются исходя из угроз, относящихся к информации о жизненном цикле документа, а также истории работы пользователей с документом. Информация о жизненном цикле документа, а также история о работе с документом представляют собой записи в таблицах баз данных. Способы защиты такой информации определяются архитектурой системы, и способах обращения к этим БД. Во многих системах отсутствуют специальные способы защиты такой информации, единственным решением является ограничение доступа пользователей к БД, однако, при наличии необходимых прав пользователь может получить доступ к записям в БД и изменить их.

Таким образом, можно сделать вывод о том, что защищенность систем ЭДО напрямую зависит от архитектуры системы и программных средств, с помощью которых она создана, применение дополнительных мер по защите информации необходимо в первую очередь для компенсации этих недостатков. В этом случае возникает вопрос об оптимальности расходования ресурсов, наиболее рациональным с точки зрения расходования затрат на защиту системы ЭДО является проектирование и реализация

необходимых для электронного документооборота, встроенных средств защиты информации: проверка целостности документов, контроль доступа к документам, блокирование действий пользователей, включая администраторов, по изменению информации о жизненном цикле документа и/или истории работы пользователей с документом.

Закладывание в архитектуру системы ЭДО внутренних механизмов по защите информации позволит, без применения дополнительных внешних технических и программных средств, гарантировать достоверность документов, контролировать все действия пользователей с документами, производить обнаружение факта фальсификации документов.

Список литературы

1. ГОСТ Р 7.0.8-2013. «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения»
2. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»
3. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
4. ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»
5. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
6. Н.Н. Куняев, А.С. Дёмашкин, А.Г. Фабричных; под общ. ред. Н.Н. Куняева Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник. – М.: Логос, 2011. – 452с. (Новая университетская библиотека)